OTOP STANDARD OPERATING PROCEDURE:
IT POLICY DEVELOPMENT AND REVIEW PROCESS

SOP

This Standard Operating Procedure (SOP) establishes a standard Information Technology Policy document hierarchy and process to guide OTOP staff and managers in developing and reviewing the appropriate type and level of information technology "policy" documents. The requirements and formats supersede all previous OTOP (or OIRM) IT policy development processes and formats. The hierarchy is based on the previously proposed OEI Policy Framework.

Purpose

The purpose of this Information Technology Policy document SOP for OTOP is to establish a tiered hierarchy and a review process for OTOP's information technology policies. An SOP will aid OTOP's "policy" writers by providing a uniform structure for planning and organizing "policy" content and defining the review and approval required for "policy" documents in each tier of the hierarchy. It also will aid customers and users by reducing the time and effort needed to find and understand "policy" information. The tiered hierarchy defines four levels of "policy" documents: Policies, Procedures, Technical Operations and Standards (TOPS), and Guidelines. **Under this structure, an OTOP "policy" document will usually have related, companion documents under one or more of the other tiers, but this is not required. Documents in Tiers 1, 2, and 3 will require mandatory compliance and/or actions. Tier 4 documents may contain guidelines and best practices, but will not require mandatory compliance.**

Content

1st Tier - Policy: An information technology Policy document is a high level statement of principles driven by statute, law, Executive Order, or the mandate of an oversight agency or Congress, and is issued to the Agency to guide management and employee decisions. In the "policy" hierarchy a Tier 1 document imposes mandatory requirements upon the entire Agency. An information technology Policy is written in a standard, agreed-upon format and uniform style which facilitate customer use and compliance. An information technology Policy must go through the Agency Directives Clearance review process or an equivalent, alternate method agreed to by the Office of Administration and Resources Management. [When an approved, alternate review process is authorized, OTOP's Policy documents will be issued by the Chief Information Officer (CIO), after first

being reviewed by the Quality and Information Council (QIC).]

2nd Tier - Procedures: A Tier 2 information technology Procedures document is normally a companion document to a Tier 1 Policy and, as such, describes the mandatory, detailed, step-by-step process to implement and comply with that information technology Policy. An information technology Procedure is written in a standard, agreed-upon format and uniform style which facilitate customer use and compliance. An information technology Procedure will usually identify specific functional outcomes, but will be technology-independent.

An information technology Procedure goes through the Agency Directives Clearance Review process or an equivalent, alternate method agreed upon by the Office of Administration and Resources Management. [When an approved, alternate review process is authorized, OTOP's Procedures documents will be issued by the CIO or such authority may be redelegated to the Office Director level. Before being approved, the Procedure would be reviewed by the appropriate QIC subcommittee(s), based upon their areas of responsibility.]

3rd Tier – Technical Operations and Standards (TOPS): A Technical Operations and Standards document is a mandatory, detailed technical document containing such things as standard configurations and operating instructions. It is a "rule/objective against which conformance can be measured in support of directive direction or position" (NTSD Operational Directive 100.06). In the "policy" hierarchy, a Tier 3 document may be a companion to a Procedures document. It is written in a standard format and style consistent with the technical information it contains, and is intended for a specific, technical community. The authority for a TOPS document is most often derived from a Policy it helps to implement. Prior to issuance, each TOPS document is reviewed by the applicable technical community. It is issued by the OTOP Director, and issuance authority may be redelegated to the Division Director level.

4th Tier - Guidelines: A Guidelines document is a collection of non-directive, non-binding information, often related to companion Policies, Procedures, and TOPS. If a Tier 4 Guidelines document does relate to higher level Tier documents, it should identify such higher level documents for clarity. Included in a Tier 4 document would be advice and examples which would likely be helpful to the customer or user based on best practices or past experience. Due to the variety and discretionary nature of Guidelines documents, the writer has more flexibility in development of the appropriate format.

Since Guidelines do not contain mandatory requirements, they are not required to go through the EPA Directives Clearance Review process. It is assumed, however, that customers will be consulted and included in reviews before Guidelines are finalized to ensure the suggestions made in them are workable. A Tier 4 document will be issued by the OTOP Director, and issuance authority may be redelegated to the Division Director level.

Exceptions: **Policies by Memorandum:** For time critical situations that require immediate action, information technology Policies may be issued by an Agency memorandum from the Agency's Chief Information Officer, the Administrator, or other formally delegated Agency authorities. However, Policies by memorandum are considered interim Policies and are usually issued for a short, fixed time frame, generally not to exceed one year. If Policies by memorandum are needed for the longer term, they should be entered into the Agency's Directives Clearance Review process concurrently with being issued.

Responsibilities: The OTOP Management Board of Directors will serve as a review body for OTOP documents that fall under the OTOP "policy" document tiered hierarchy (see attached flow charts **[to be added later]**). The Board of Directors consists of the OTOP Office Director, Deputy Office Director, Division Directors, and Associate Division Directors. The Board will review such draft documents before they are sent for reviews external to OTOP.

OTOP Board or Directors Review Process:

1. When the responsible Division believes a "policy"document is ready for external review, they forward it electronically to all OTOP Board of Directors members at least 2 weeks before an OTOP Board of Directors meeting.

2. The OTOP Board of Directors members review the "policy" document and at least 3 days before the meeting, contact the owning Division to either concur or indicate areas of dissent.

3. If all OTOP Board of Directors members concur with the "policy" document it can be sent forward by the responsible Division to external review.

4. If there is any dissent, the "policy" document will be discussed at the OTOP Board of Directors meeting. The goal of that discussion is to reach consensus at the meeting on changes required so the "policy" document can be sent to external review. The OTOP Director will make the final decision on whether consensus is reached and whether the document can go to external review.

5. The IT Policy and Planning Division will hold the official records relating to all OTOP "policy" documents, including development papers and records of review, clearance, decisions, and approval. ITPPD will ensure all OTOP "policy" documents are "published" so Agency staff and managers are aware of them.

"Policy" documents for which OTOP has responsibility to develop, maintain, and sunset cover a wide range of information technology topics. No one OTOP Division has exclusive responsibilities over a particular Tier and the "policy" document(s) it may require. Generally, however, it is usually the responsibility of ITPPD to identify and develop Agency Tier 1 IT Policies. Based on Division responsibilities, and through the "policy" coordination and review process, the area of responsibility for IT Policy (Tier 1) development should be apparent. If there is any question or disagreement, the determination of responsibility for development of a Tier 1 Policy will be determined by the OTOP Management Board of Directors.

During the development of a Tier 1 Policy, the need for specific types of supporting documentation is usually determined. The Tier 1 Policy should indicate which Procedures, TOPS, or Guidelines will be written in support of that Tier 1 Policy. The responsibility for writing the Tier 2 - 4 documents should be determined and assigned as soon as possible during Tier 1 Policy development. Generally it will be the responsibility of HDSD and NTSD to identify and develop Tiers 2 - 4 documents.

Tier 1 Policies generally should NOT go through other reviews (e.g., OEI, technical experts, Directives Clearance Review, etc.) until the necessary Tier 2 - 4 document(s) are identified and an OTOP Division assigned responsibility for developing them.

It is anticipated that many more Tier 2 - 4 documents than Tier 1 documents will be required. The Division responsible for the development and maintenance of supporting documents shall identify in each document the Tier 1 Policy they support, if applicable, and follow the format and review process established.
When a **workgroup** is created to develop a document that falls under the

OTOP "policy" document tiered hierarchy, a summary explaining the purpose, membership, major issues, and milestones should be provided to the OTOP Management Board of Directors.

Each Division should provide the OTOP Management Board of Directors with a brief monthly status report of each IT "policy" activity it has underway, including the status of Workgroup activities.

Authorities: **For Policies and Procedures**, final sign-off and approval authority resides with the Assistant Administrator for Administration and Resources Management or a redelegated official. If an equivalent, alternate method for OEI has been agreed upon by the Office of Administration and Resources Management, the CIO, or delegatee, shall have final sign-off and approval authority.

Technical Operations and Standards are to be signed by the OTOP Director level or whomever has been redelegated authority to approve and sign.

Guidelines are signed by the OTOP Director or whomever has been redelegated authority to approve and sign.

Any redelegations are to be made in writing.

Format: All information technology "policy" documents should conform to the requirements of the standard, OEI-proposed information policy format (see Attachment A).

Attachment A
Format for documents in Tiers 1- 3

NOTE: The proposed format for Policy and Procedures documents is the same for both OARM-approved documents and CIO-approved documents. The only difference in format is that the CIO issued Policies and Procedures will have the following OEI heading and have a CIO approval section. Otherwise, both formats are identical.

U.S. EPA

Office of Environmental Information (16)

Information Policy (20 pt)
from the Chief Information Officer (16 pt)

(16 pt)**CIO Policy No. 00-001-OIAA**

- (first two digits identify year,
- second three are numerical sequence number to be issued by OPRO, and the
- third series identifies the issuing OEI office)

Supersedes (O): Use this heading only when the policy replaces an earlier one

Issue Date:
Review Date:

R = Required, O = Optional
Font size is 12 pt

Subject (R): A short phrase which summarizes the topic being addressed.

Purpose (R): Explains the reasons for issuing the policy.

Audience (R): Identifies the EPA office or persons who are most impacted by this policy.

Background(R): This section describes the events or circumstances which make it necessary to issue this policy.

Authorities (R): Lists the documents (laws, memorandums, OMB circulars, etc) which initiate, require and/or enforce the policy. Include the URL, if available, for each document.

Related Documents (O): These are other materials which provide insight and background information about the policy. (This is an optional heading.)

Policy (R): Statements which spell out the required actions in plain language.

Roles and Responsibilities (R): Lists the assignments of EPA individuals that will make the policy effective.

Definitions (O): Provides the meaning of terms used in the policy which are not commonly used. (This is an optional heading.)

Recertification Date (R): A date in the future by which the policy must be reviewed and reissued. This heading is intended to preclude obsolete policies.

Additional Information (R): The name, office, phone number, and email address of the individual to whom questions may be directed.

Approval (R): The signature and name of the CIO who is issuing the policy, and the date of signature.

Chief Information Officer Date